Site-to-Site-VPN-Konfiguration auf FTD, von FMC verwaltet

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration von Site-to-Site-VPN auf FirePOWER Threat Defense (FTD), das von FMC verwaltet wird.

Voraussetzungen

Anforderungen

Sie sollten über Kenntnisse in den folgenden Themen verfügen:

- Grundlegendes Verständnis von VPN
- Erfahrung mit FirePOWER Management Center
- Erfahrung mit der ASA-Kommandozeile

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco FTD 6.5
- ASA 9.10(1)32
- IKEv2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfiguration

Beginnen Sie mit der Konfiguration auf FTD mit FirePower Management Center.

Schritt 1: Definieren der VPN-Topologie

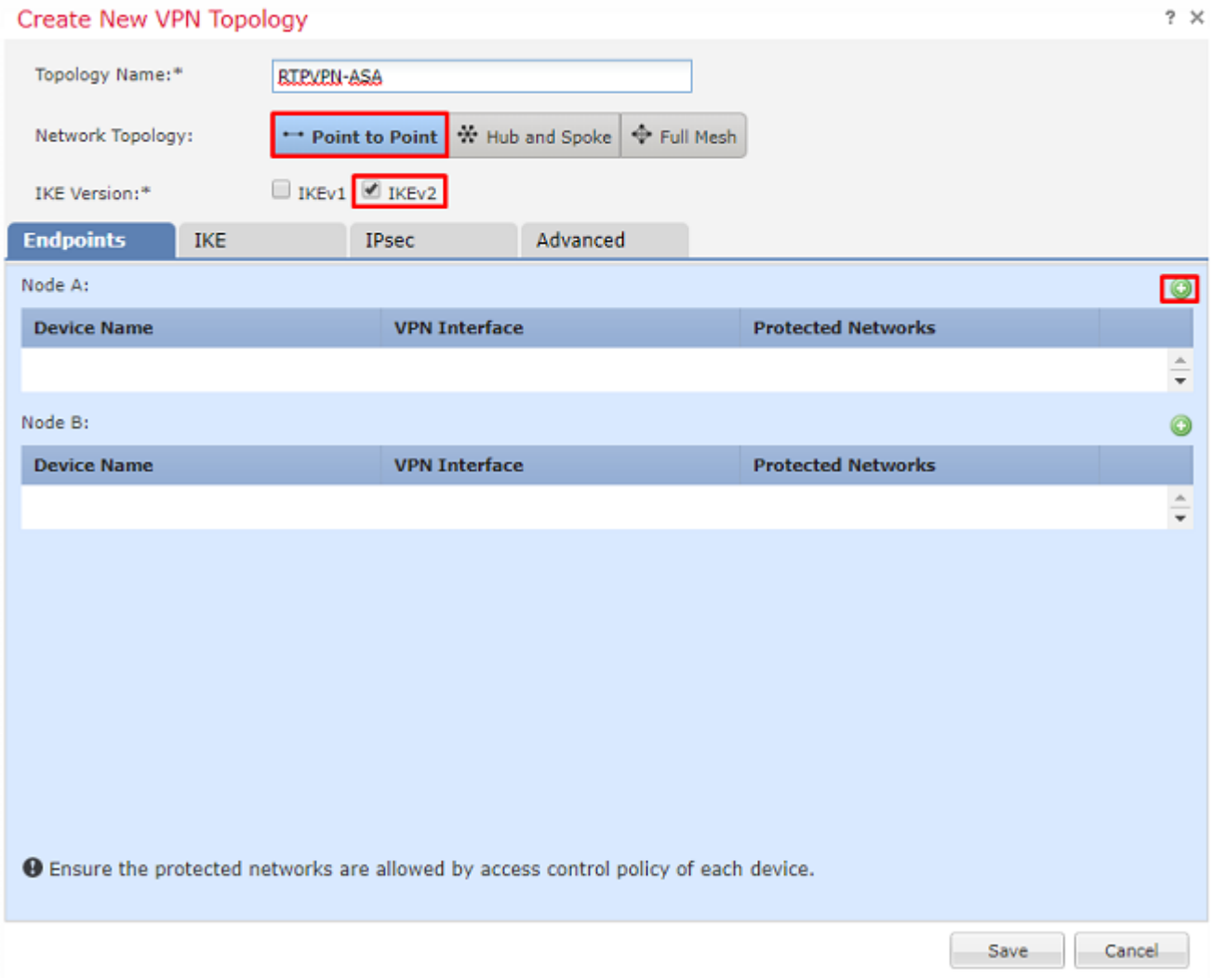
1. Navigieren Sie zu **Geräte > VPN > Site-to-Site.** Klicken Sie unter "VPN hinzufügen" auf **Firepower Threat Defense Device**, wie in dieser Abbildung dargestellt.

2. Das Feld "**Neue VPN-Topologie erstellen**" wird angezeigt. Geben Sie VPN einen leicht identifizierbaren Namen.

Netzwerktopologie: Point-to-Point

IKE-Version: IKEv2

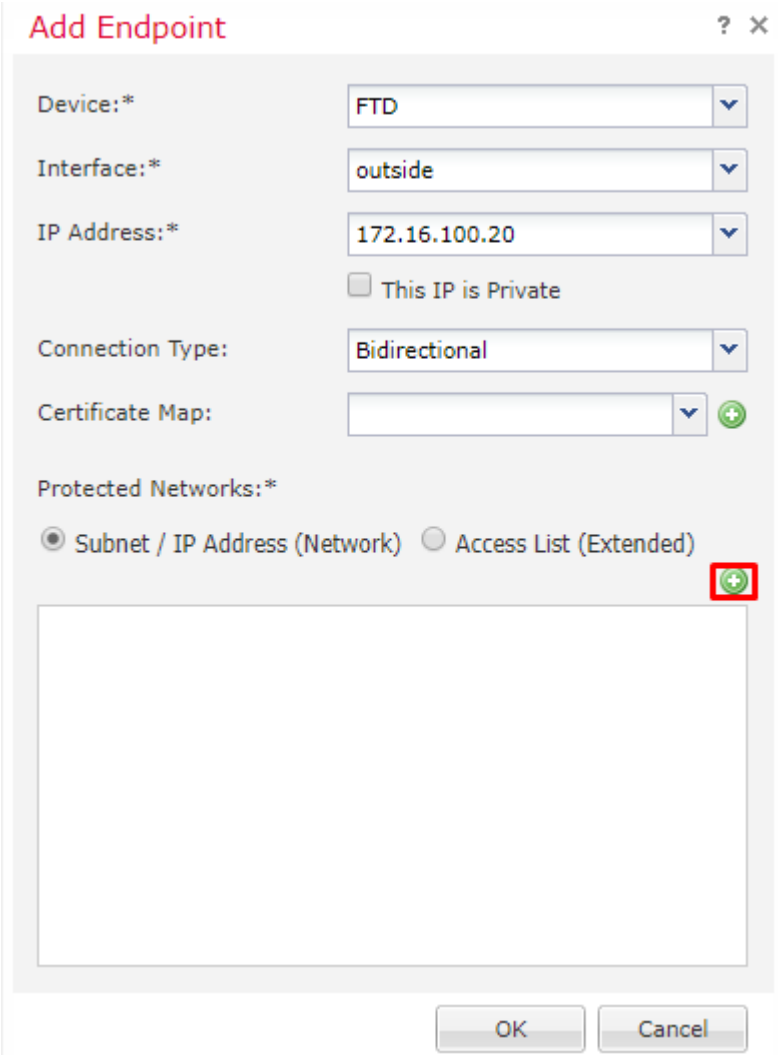
Wenn Sie in diesem Beispiel Endpunkte auswählen, ist Knoten A die FTD und Knoten B die ASA. Klicken Sie auf das grüne Pluszeichen, um Geräte zur Topologie hinzuzufügen, wie in diesem Bild gezeigt.



3. Fügen Sie die FTD als ersten Endpunkt hinzu.

Wählen Sie die Schnittstelle aus, auf der eine Crypto Map platziert wird. Die IP-Adresse sollte automatisch aus der Gerätekonfiguration übernommen werden.

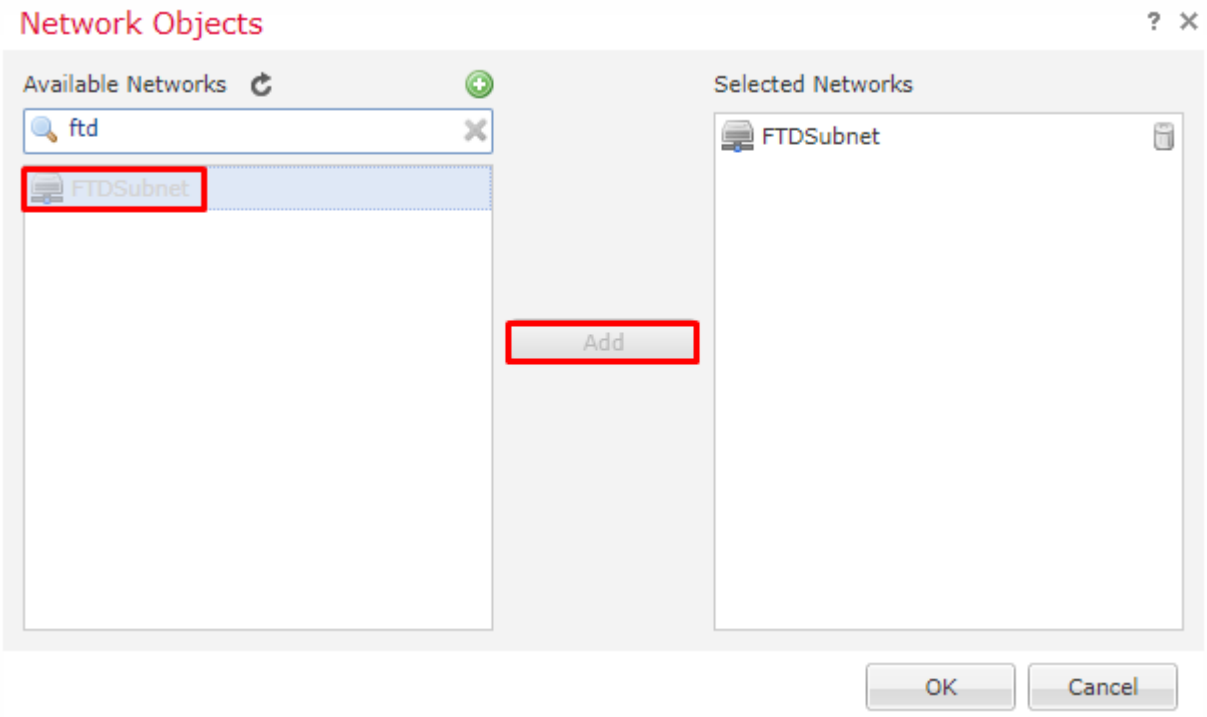
Klicken Sie auf das grüne Pluszeichen unter "Protected Networks" (Geschützte Netzwerke), wie in diesem Bild dargestellt, um auszuwählen, welche Subnetze in diesem VPN verschlüsselt werden sollen.



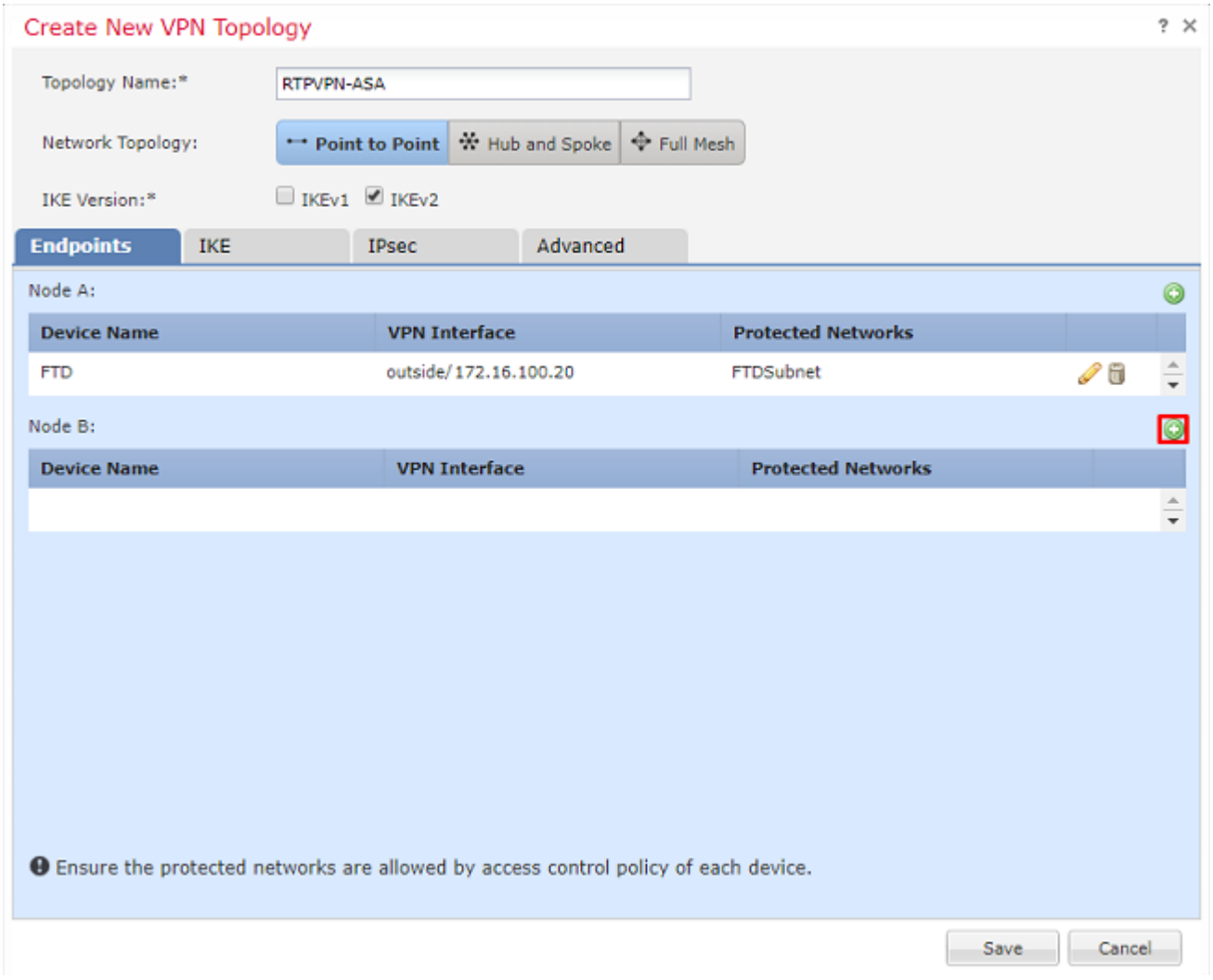
4. Klicken Sie auf grün plus und hier wird ein Netzwerkobjekt erstellt.

5. Fügen Sie alle lokalen Subnetze zum FTD hinzu, die verschlüsselt werden müssen. Klicken Sie auf **Hinzufügen**, um sie in die Liste "Ausgewählte Netzwerke" zu verschieben. Klicken Sie nun auf **OK**, wie in diesem Bild dargestellt.

FTDSubnet = 10,10.113.0/24

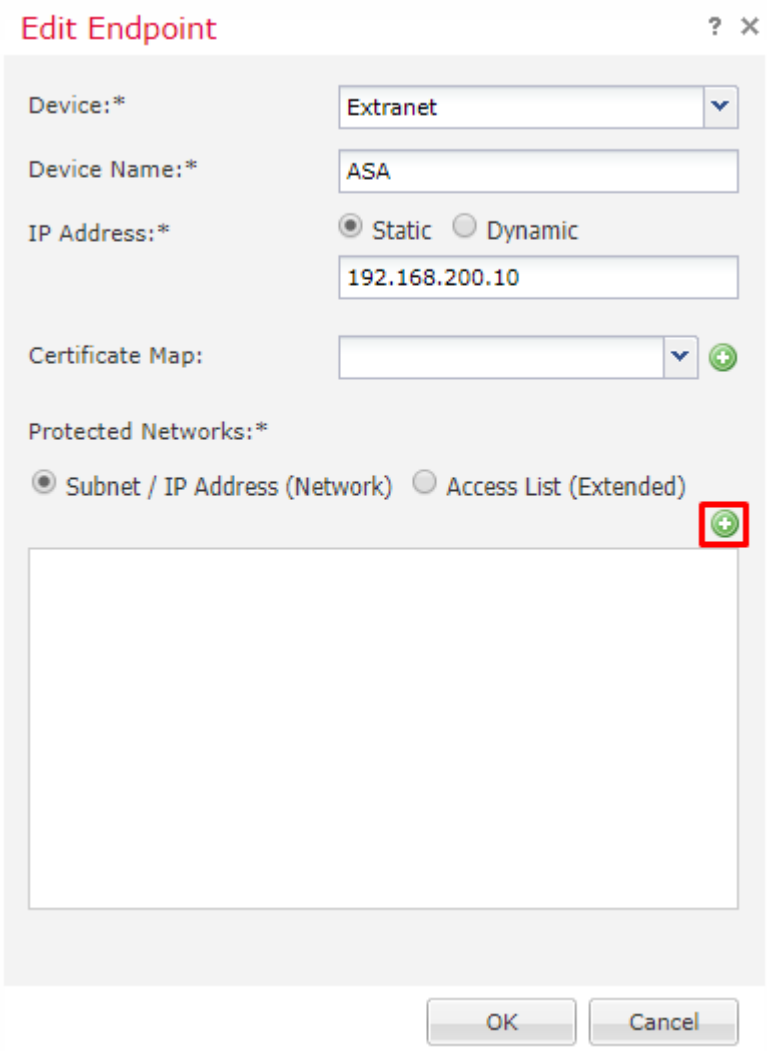


Knoten A: (FTD)-Endpunkt ist abgeschlossen. Klicken Sie auf das grüne Pluszeichen für Knoten B, wie im Bild dargestellt.



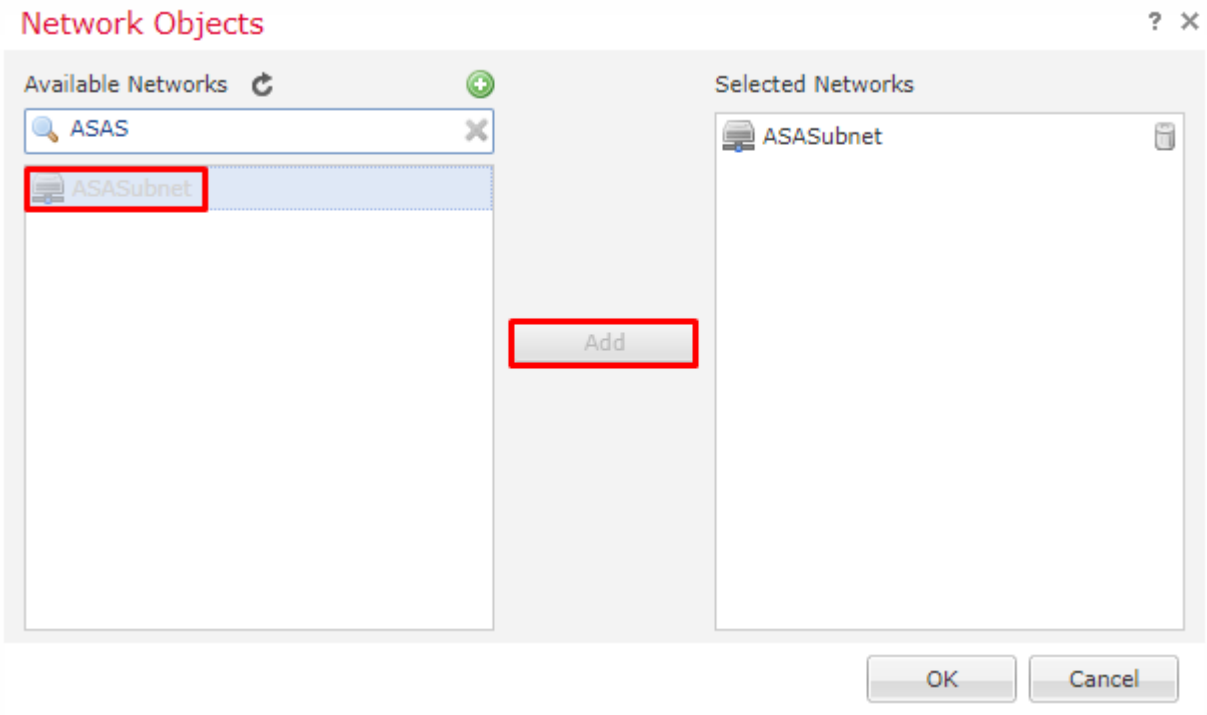
Knoten B ist eine ASA. Geräte, die nicht vom FMC verwaltet werden, gelten als Extranet.

6. Fügen Sie einen Gerätenamen und eine IP-Adresse hinzu. Klicken Sie auf das grüne Pluszeichen, um geschützte Netzwerke hinzuzufügen, wie im Bild gezeigt.



7. Wählen Sie, wie in diesem Bild dargestellt, die zu verschlüsselnden **ASA-Subnetze aus**, und fügen Sie sie den ausgewählten Netzwerken hinzu.

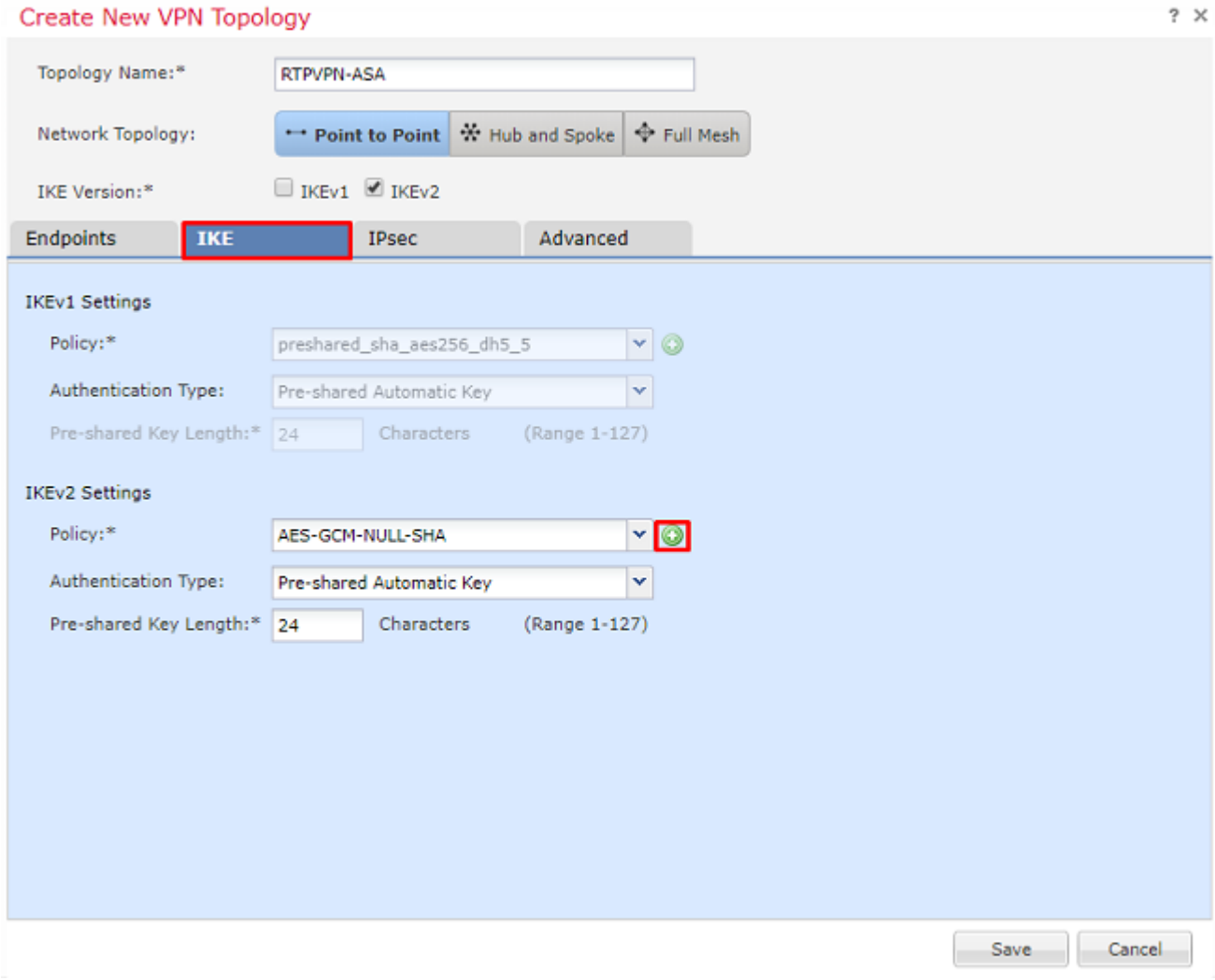
ASASubnet = 10,10.110.0/24



Schritt 2: Konfigurieren der IKE-Parameter

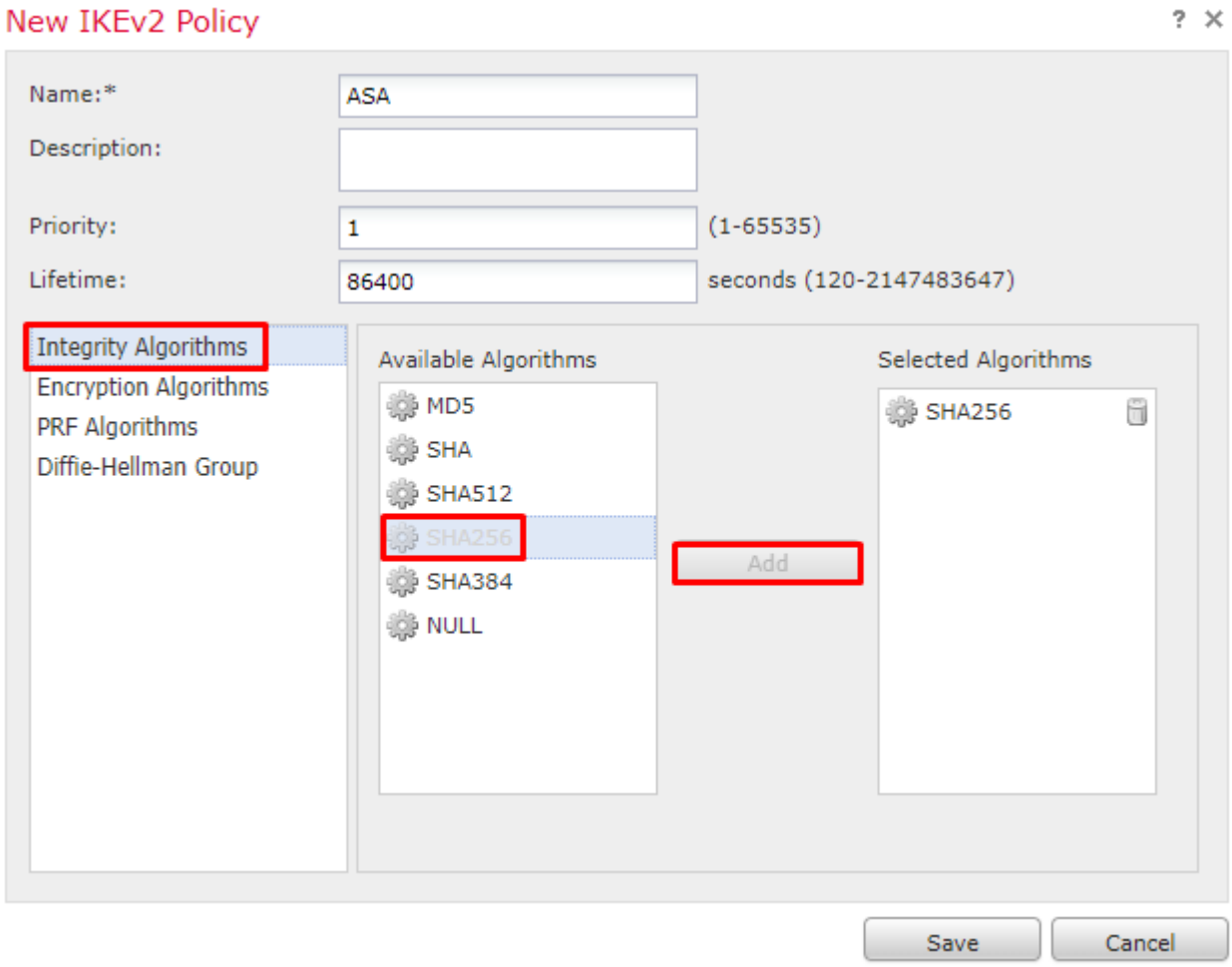
Beide Endpunkte durchlaufen jetzt die IKE/IPSEC-Konfiguration.

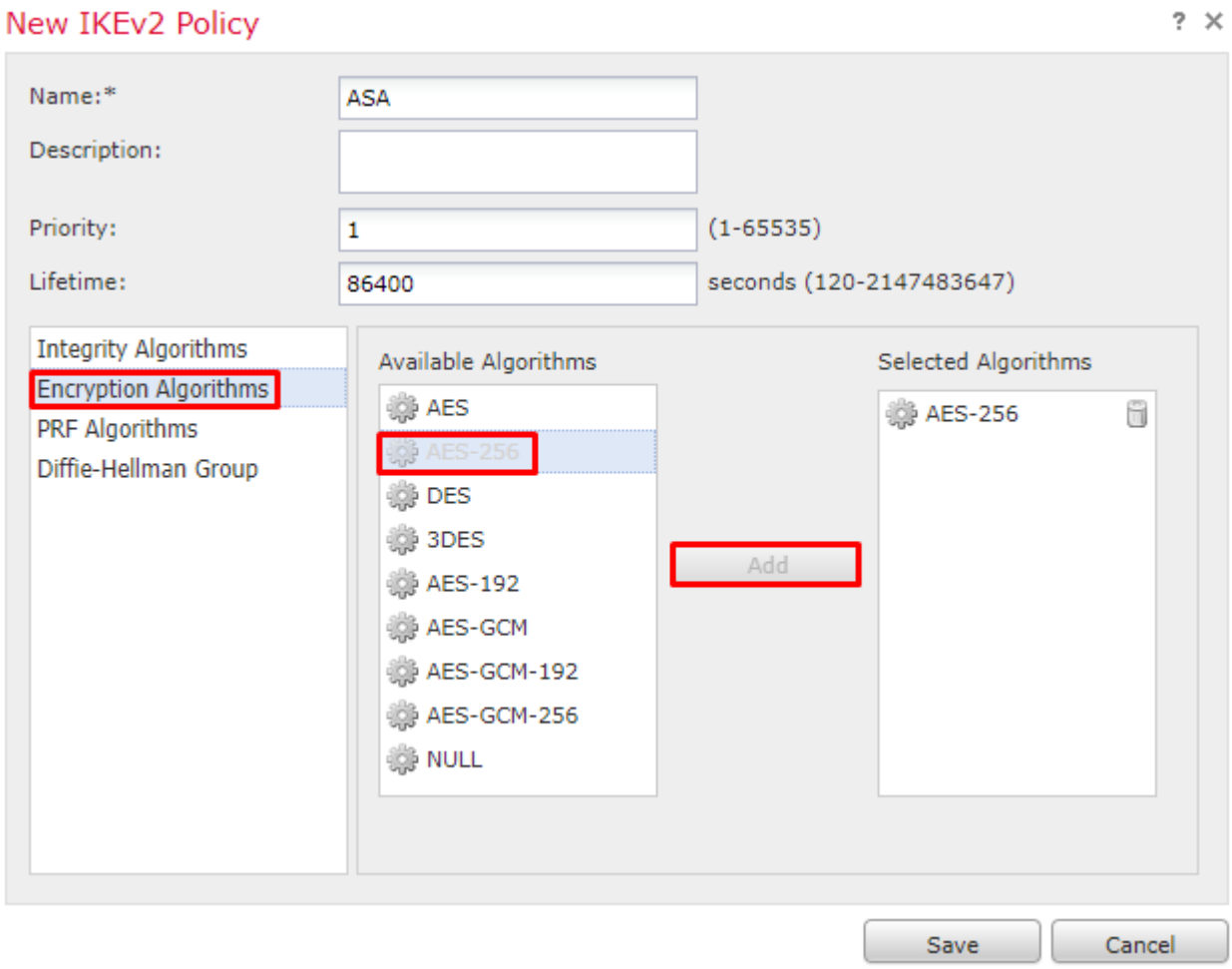
1. Geben Sie auf der Registerkarte **IKE** die Parameter an, die für den IKEv2-Erstaustausch verwendet werden. Klicken Sie auf das grüne Pluszeichen, um eine neue IKE-Richtlinie zu erstellen, wie im Bild gezeigt.

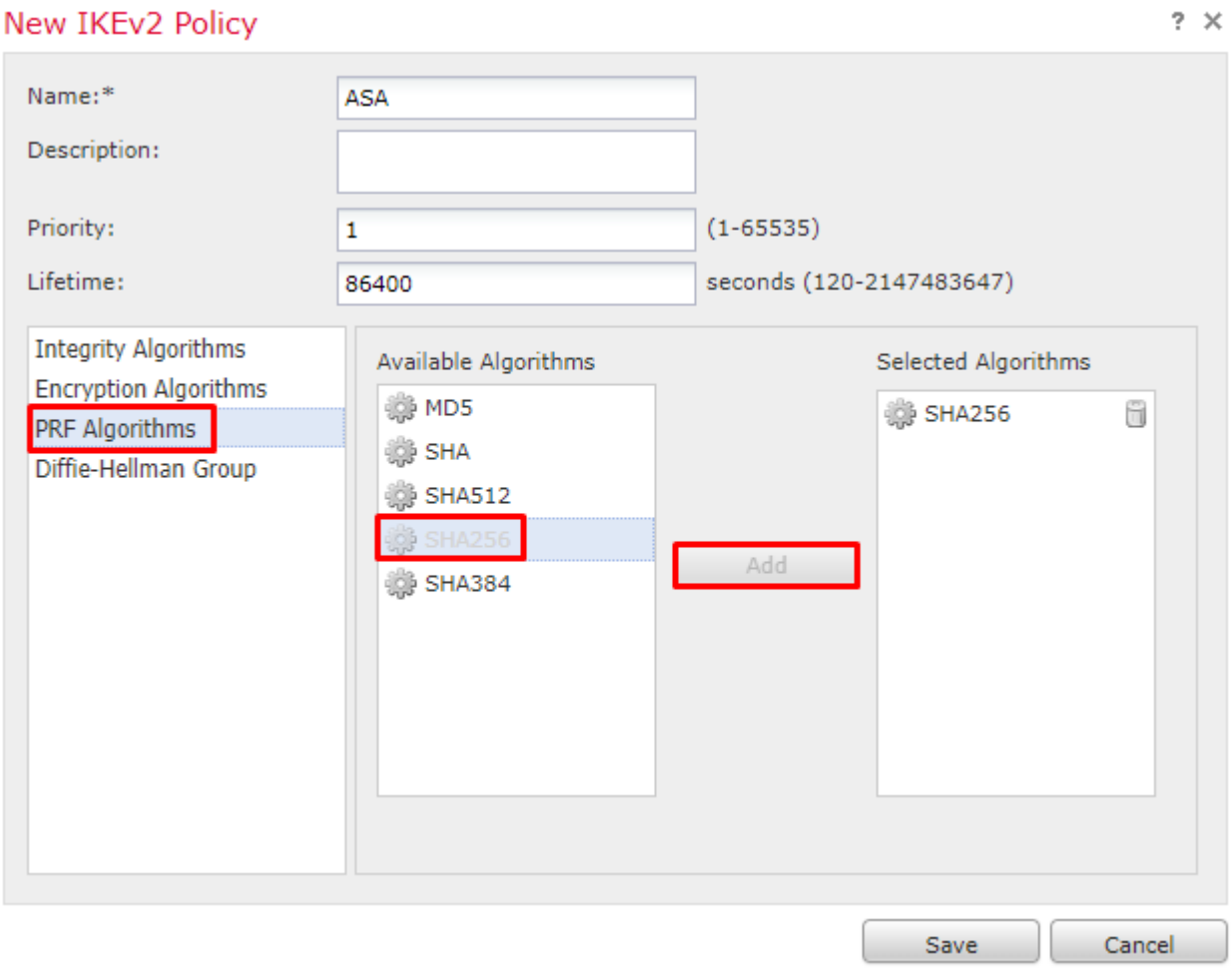


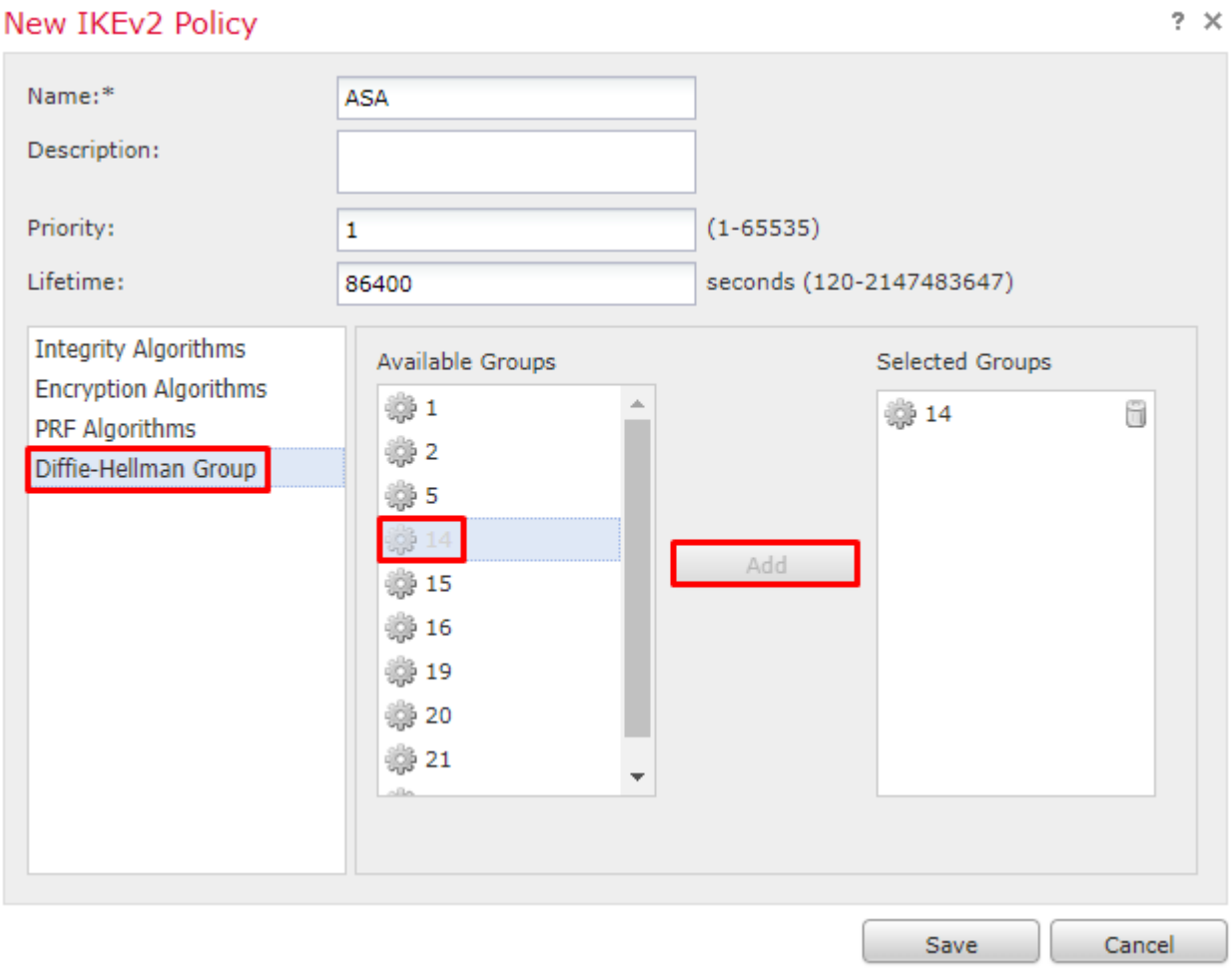
2. Geben Sie in der neuen IKE-Richtlinie eine Prioritätsnummer sowie die Lebensdauer von Phase 1 der Verbindung an. In diesem Dokument werden folgende Parameter für den ersten Austausch verwendet: Integrity (SHA256), Encryption (AES-256), PRF (SHA256) und Diffie-Hellman Group (Group 14).

Hinweis: Alle IKE-Richtlinien auf dem Gerät werden an den Remote-Peer gesendet, unabhängig davon, was im ausgewählten Richtlinienabschnitt enthalten ist. Die erste IKE-Richtlinie, der der Remote-Peer entspricht, wird für die VPN-Verbindung ausgewählt. Wählen Sie mithilfe des Prioritätsfelds aus, welche Policy zuerst gesendet werden soll. Priorität 1 wird zuerst gesendet.


New IKEv2 Policy
Name:*
ASA
Description:
Priority:
1
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
MD5
SHA
SHA512
SHA256
SHA384
NULL
Add
Selected Algorithms
SHA256
Save
Cancel

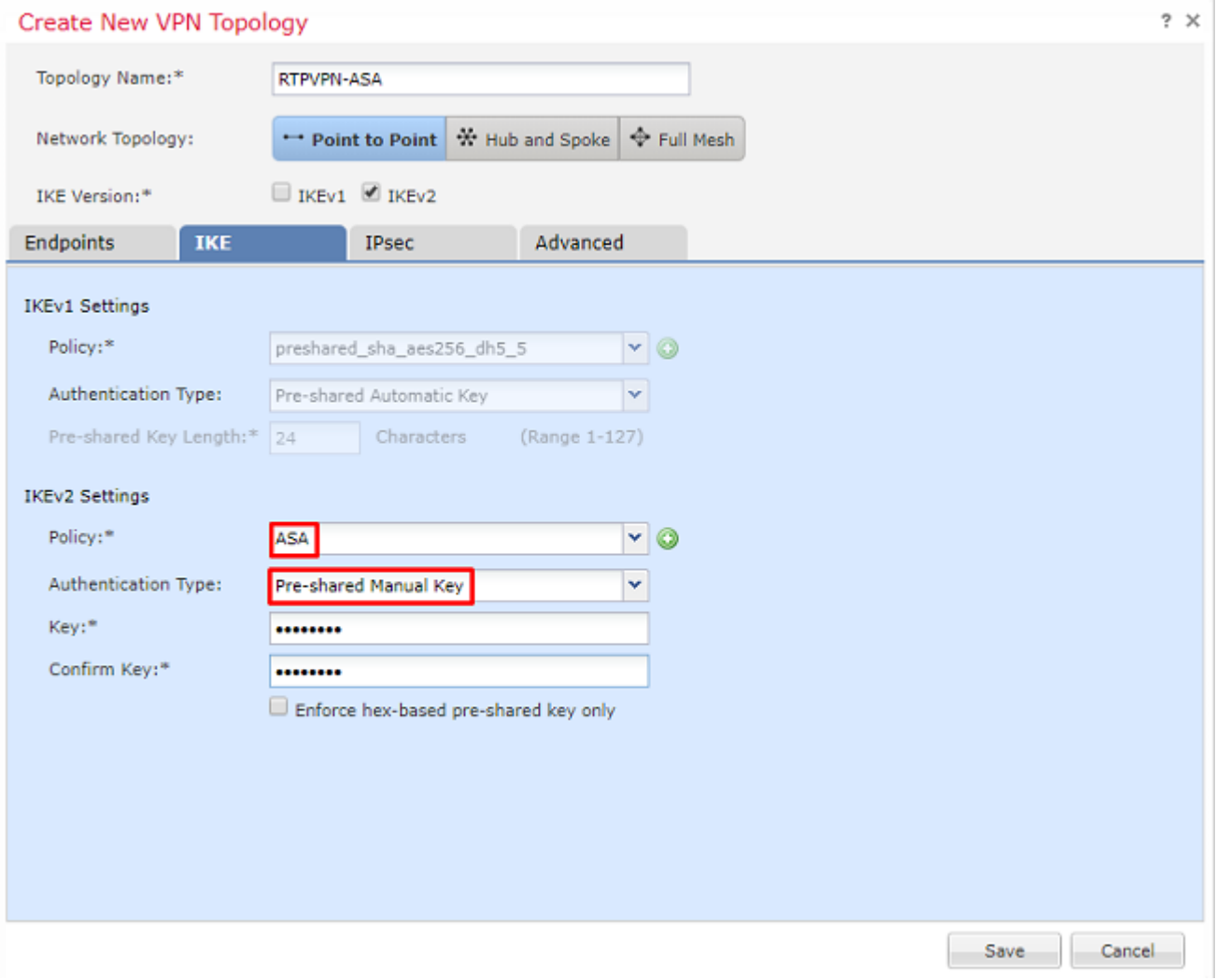

New IKEv2 Policy
Name:*
ASA
Description:
Priority:
1
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
AES
AES-256
DES
3DES
AES-192
AES-GCM
AES-GCM-192
AES-GCM-256
NULL
Add
Selected Algorithms
AES-256
Save
Cancel


New IKEv2 Policy
Name:*
ASA
Description:
Priority:
1
(1-65535)
Lifetime:
86400
seconds (120-2147483647)
Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group
Available Algorithms
MD5
SHA
SHA512
SHA256
SHA384
Add
Selected Algorithms
SHA256
Save
Cancel



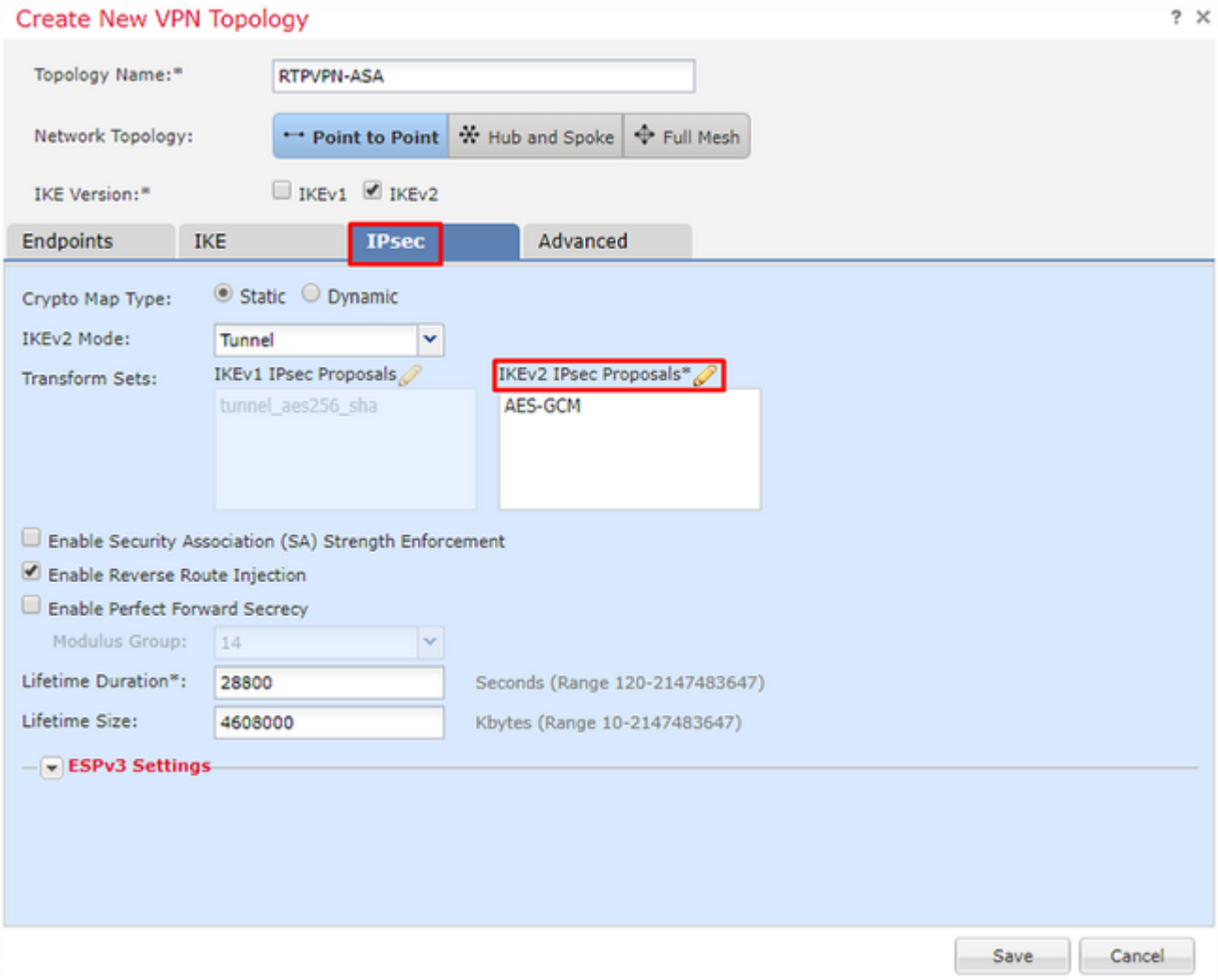
3. Nachdem die Parameter hinzugefügt wurden, wählen Sie diese Richtlinie und dann den **Authentifizierungstyp aus**.

4. Wählen Sie **Pre-Shared-Key** Manual. Für dieses Dokument wird der PSK cisco123 verwendet.



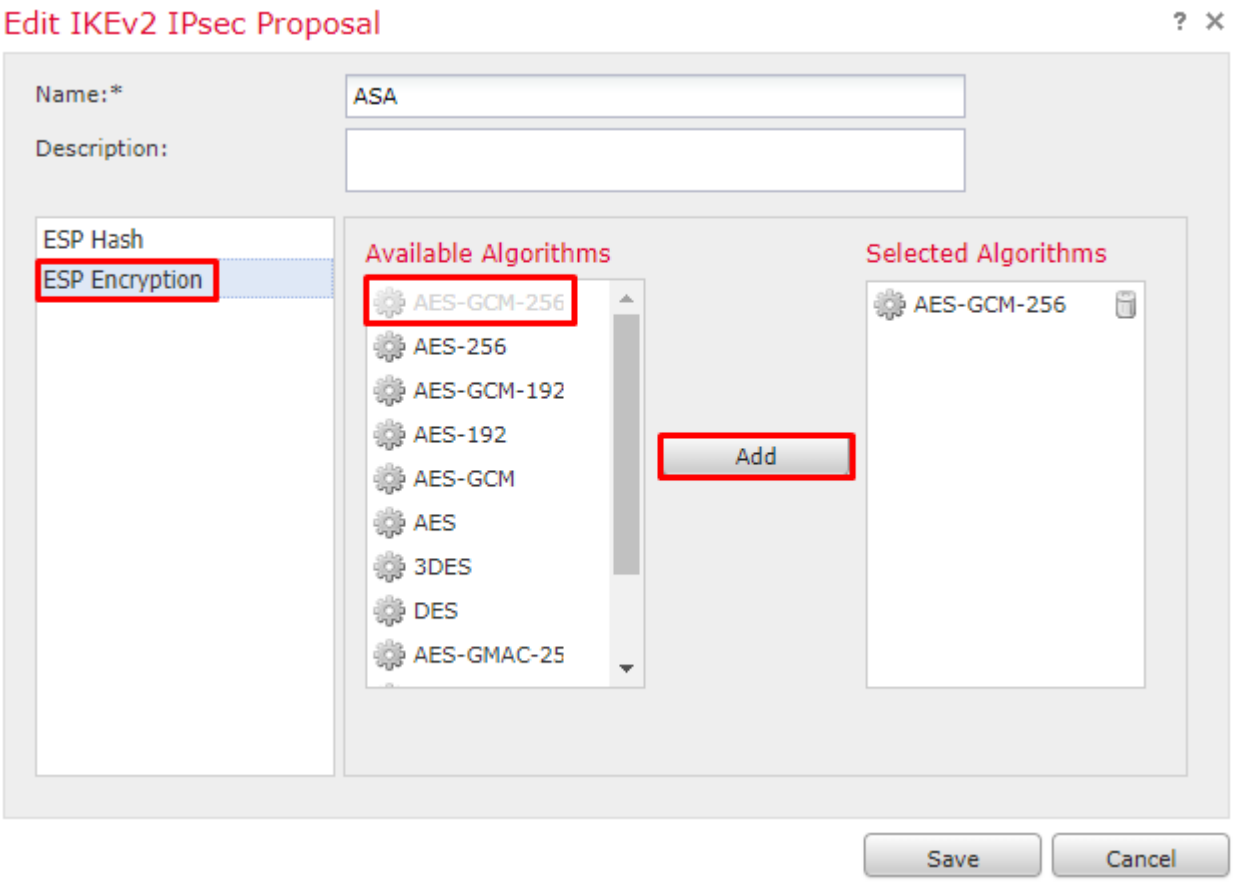
Schritt 3: Konfigurieren von IPsec-Parametern

1. Klicken Sie unter **IPsec** auf den Bleistift, um den Transformationssatz zu bearbeiten und einen neuen IPsec-Vorschlag zu erstellen, wie in diesem Bild dargestellt.

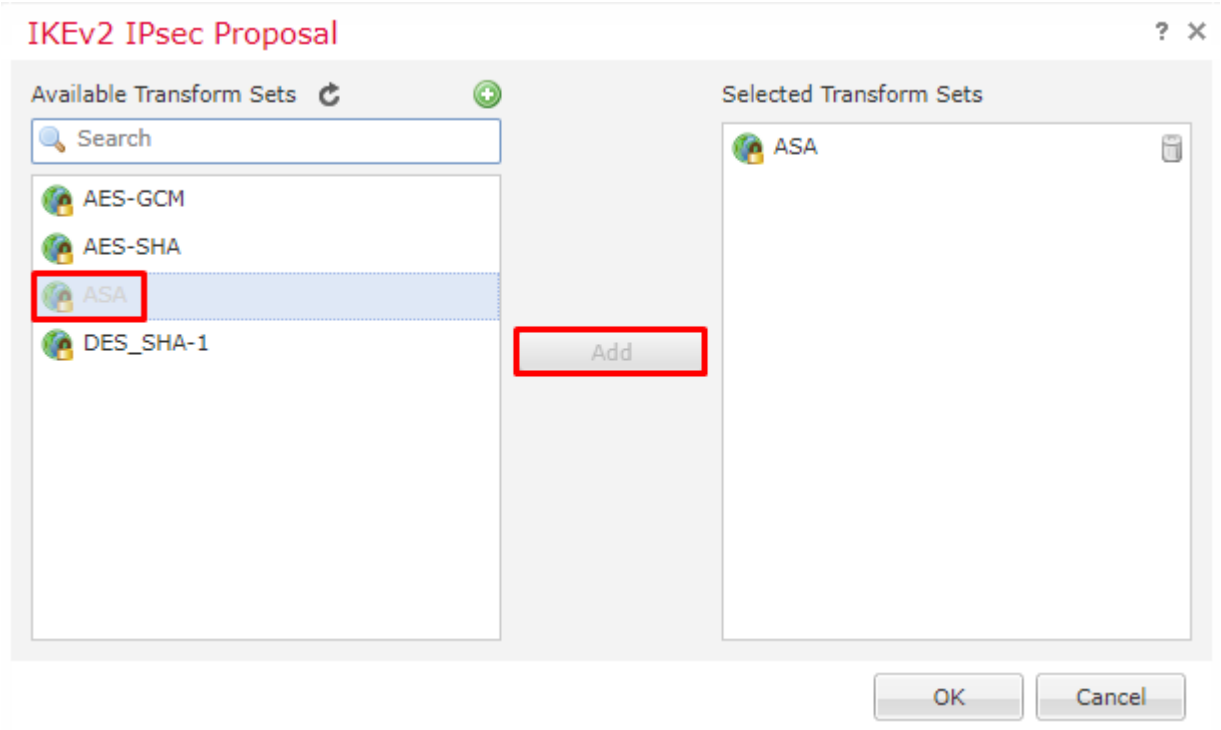


2. Klicken Sie auf das grüne Pluszeichen, und geben Sie die Parameter für Phase 2 ein, um einen neuen IKEv2-IPsec-Vorschlag zu erstellen.

Wählen Sie **ESP Encryption > AES-GCM-256 aus**. Wenn der GCM-Algorithmus für die Verschlüsselung verwendet wird, ist kein Hash-Algorithmus erforderlich. Mit GCM ist die Hash-Funktion integriert.

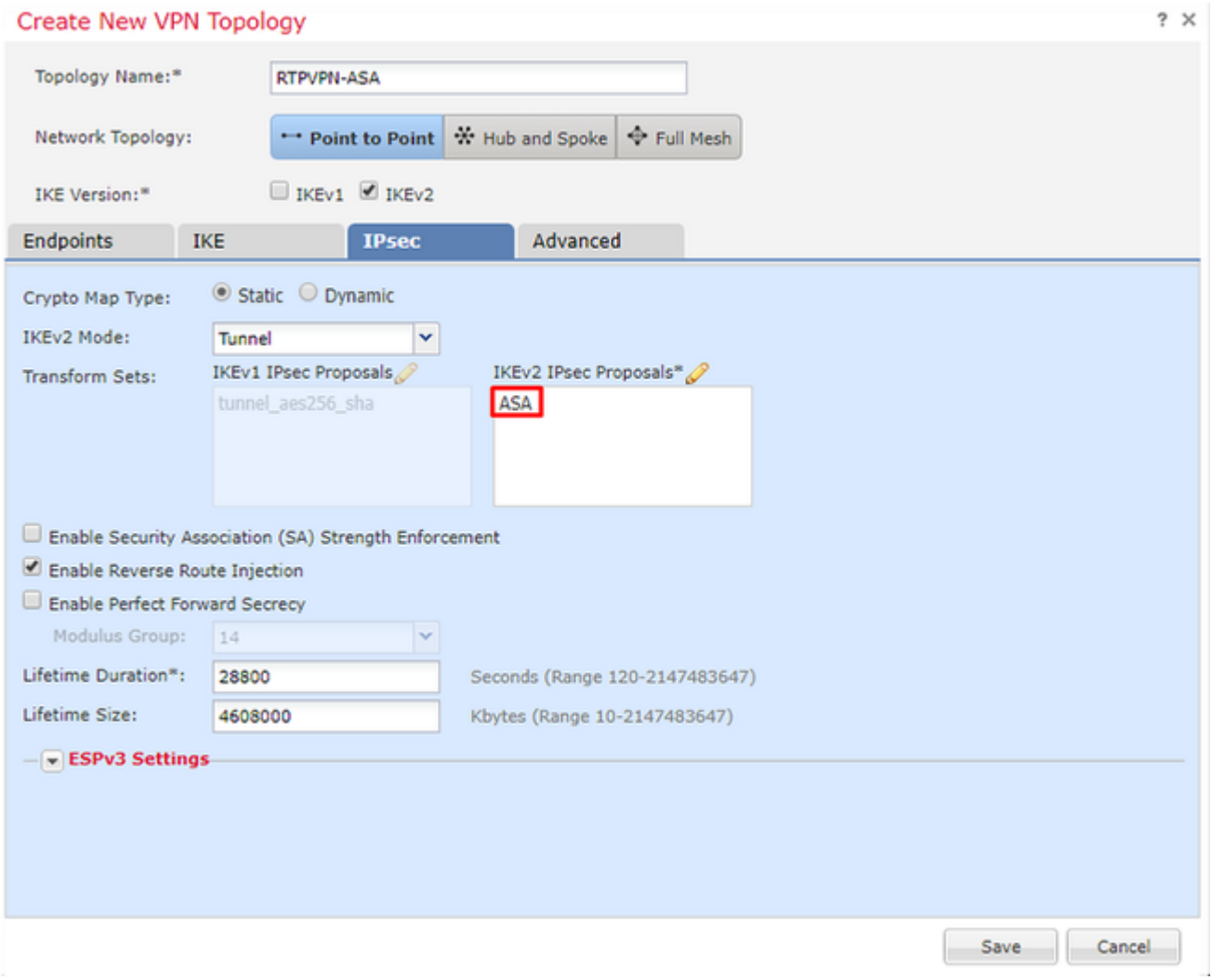


3. Nachdem der neue IPsec-Vorschlag erstellt wurde, fügen Sie ihn den ausgewählten Transformationssätzen hinzu.



Der neu ausgewählte IPsec-Vorschlag wird jetzt unter den IKEv2-IPsec-Vorschlägen aufgeführt.

Hier können bei Bedarf die Lebensdauer von Phase 2 und PFS bearbeitet werden. In diesem Beispiel wird die Lebensdauer als Standard festgelegt und PFS deaktiviert.

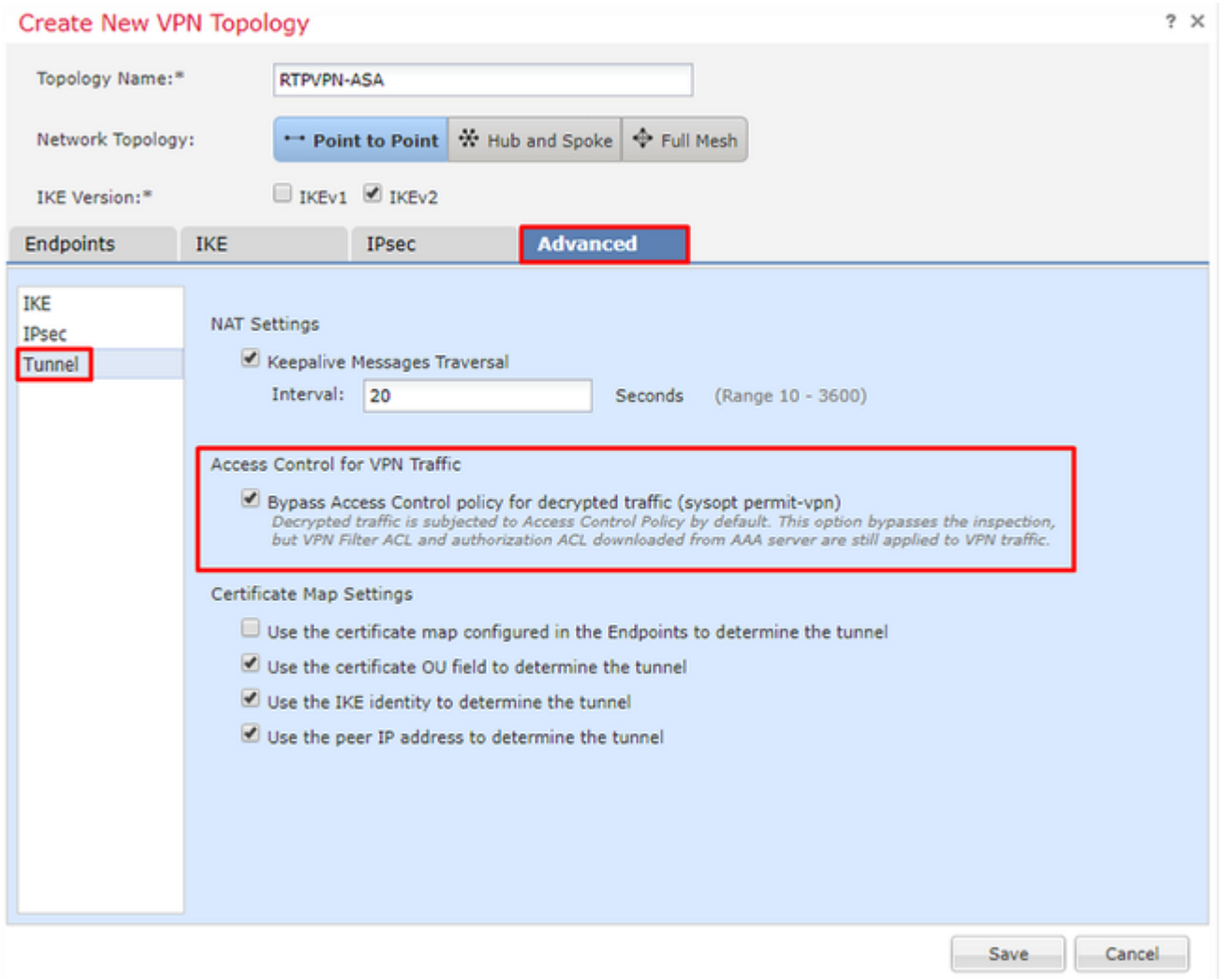


Optional - Sie müssen entweder die Option zum Umgehen der Zugriffskontrolle ausführen oder eine Zugriffskontrollrichtlinie erstellen.

Schritt 4: Zugriffskontrolle umgehen.

Optional kann **sysopt permit-vpn** unter **Erweitert > Tunnel** aktiviert werden.

Damit entfällt die Möglichkeit, den von den Benutzern eingehenden Datenverkehr mithilfe der Zugriffskontrollrichtlinie zu überprüfen. VPN-Filter oder herunterladbare ACLs können weiterhin verwendet werden, um den Benutzerdatenverkehr zu filtern. Hierbei handelt es sich um einen globalen Befehl, der auf alle VPNs angewendet wird, wenn dieses Kontrollkästchen aktiviert ist.

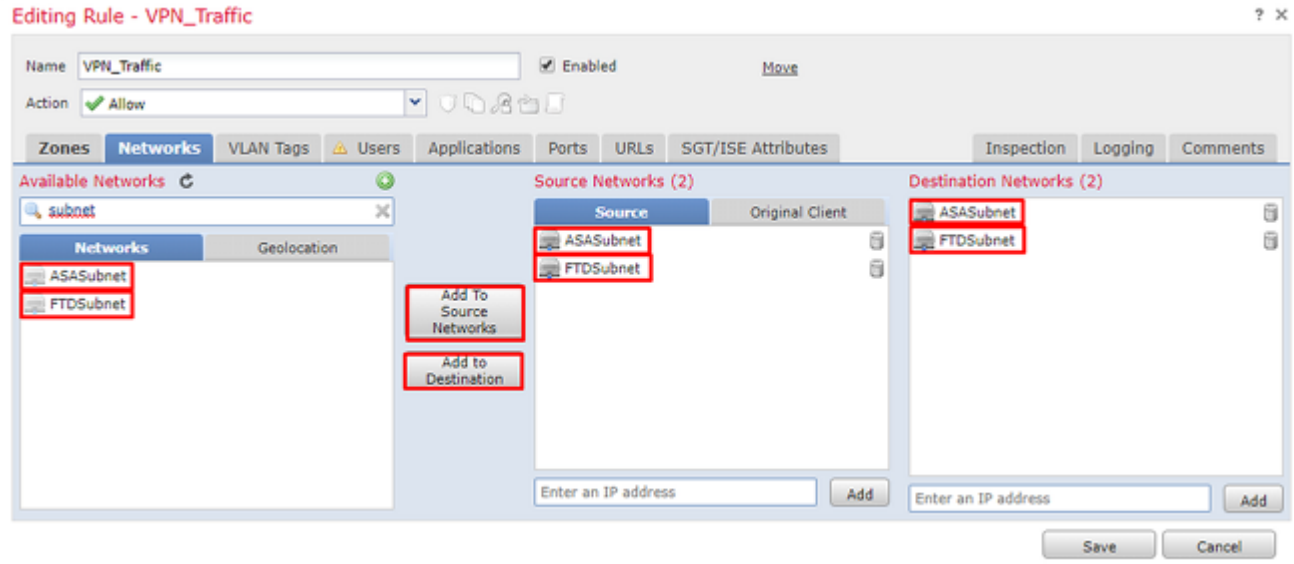


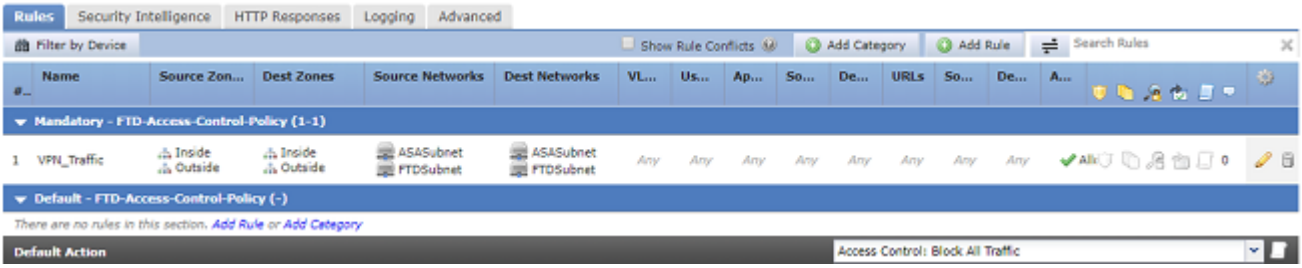
Wenn **sysopt permit-vpn** nicht aktiviert ist, muss eine Zugriffskontrollrichtlinie erstellt werden, um den VPN-Datenverkehr über das FTD-Gerät zuzulassen. Wenn **sysopt permit-vpn** aktiviert ist, überspringen Sie die Erstellung einer Zugriffskontrollrichtlinie.

Schritt 5: Erstellen einer Zugriffskontrollrichtlinie

Navigieren Sie unter Zugriffskontrollrichtlinien zu **Richtlinien > Zugriffskontrolle > Zugriffskontrolle,** und wählen Sie die Richtlinie aus, die auf das FTD-Gerät abzielt. Um eine Regel hinzuzufügen, klicken Sie auf **Regel hinzufügen**, wie in der Abbildung dargestellt.

Der Datenverkehr muss vom internen Netzwerk zum externen Netzwerk und vom externen Netzwerk zum internen Netzwerk zugelassen werden. Erstellen Sie eine Regel, um beides gleichzeitig auszuführen, oder erstellen Sie zwei Regeln, um sie getrennt zu halten. In diesem Beispiel wird eine Regel erstellt, die beides ermöglicht.

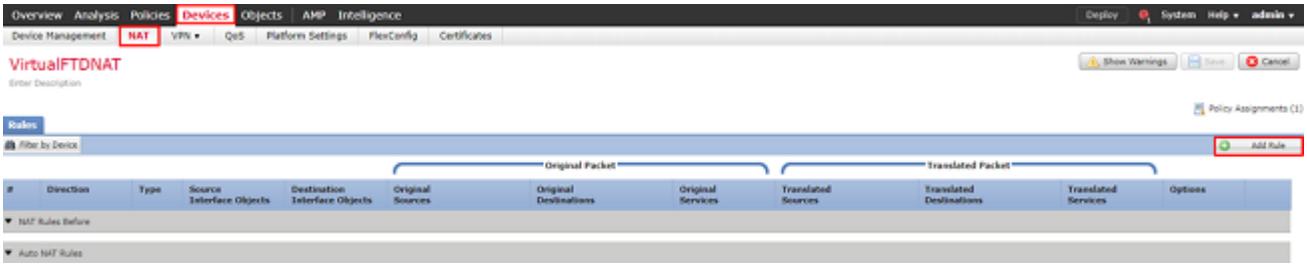




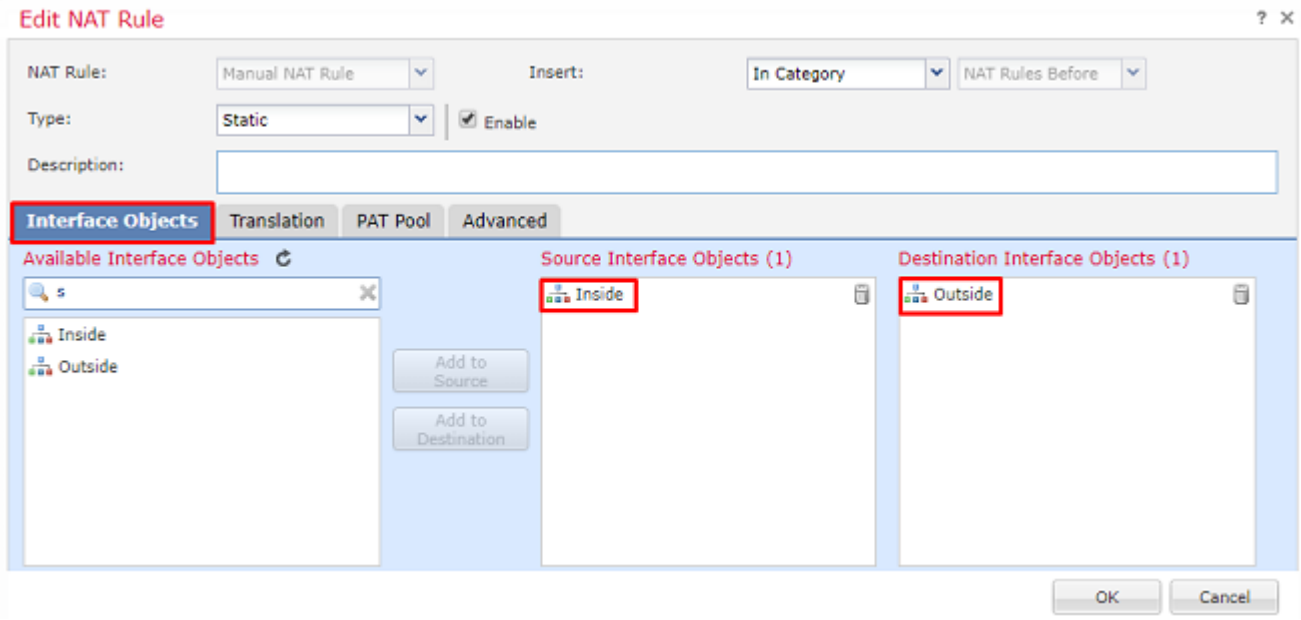
Schritt 6: Konfigurieren Sie die NAT-Ausnahme.

Konfigurieren Sie eine NAT Exemption-Anweisung für den VPN-Verkehr. Eine NAT-Ausnahme muss vorhanden sein, damit VPN-Datenverkehr nicht auf eine andere NAT-Anweisung trifft und VPN-Datenverkehr nicht falsch übersetzt wird.

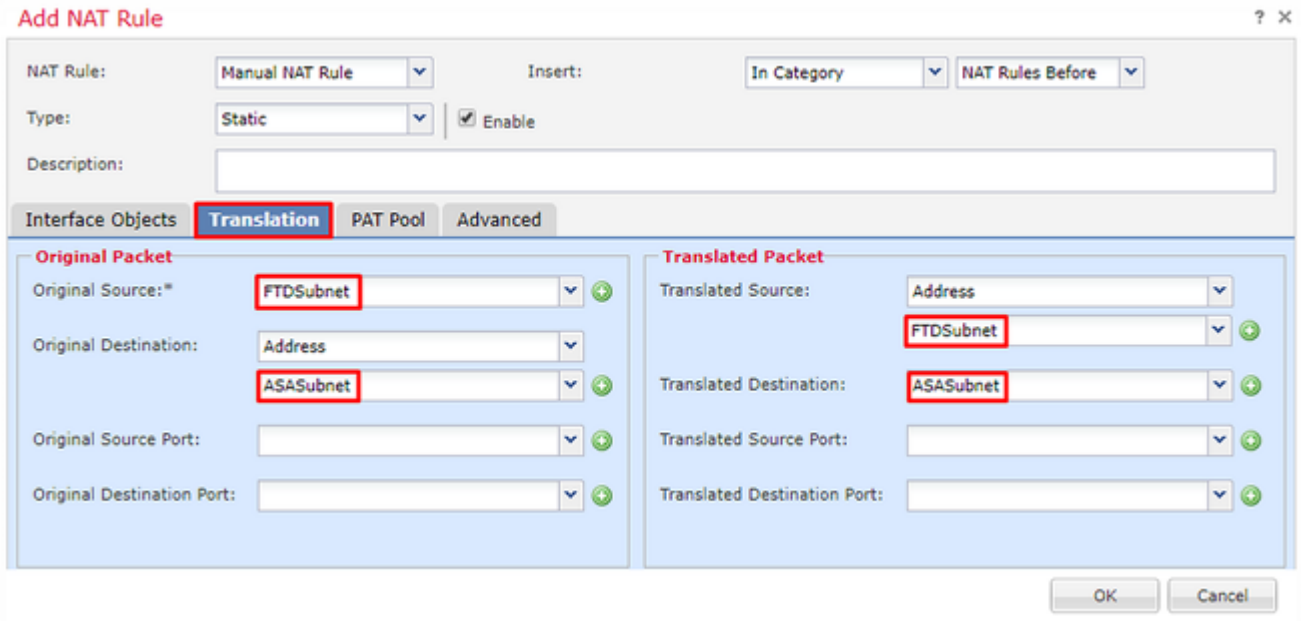
1. Navigieren Sie zu **Devices (Geräte) > NAT**, und wählen Sie die NAT-Richtlinie aus, die auf das FTD abzielt. Erstellen Sie eine neue Regel, indem Sie auf die Schaltfläche **Regel hinzufügen** klicken.



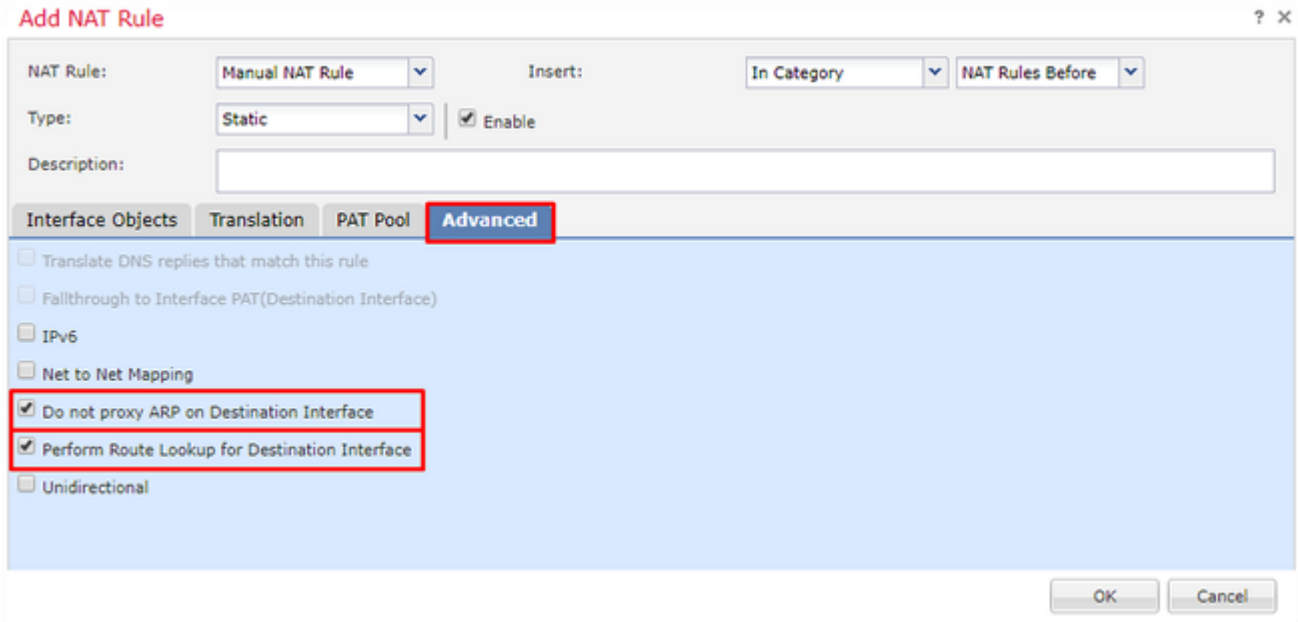
2. Erstellen einer neuen statischen manuellen NAT-Regel Verweisen Sie auf die internen und externen Schnittstellen.



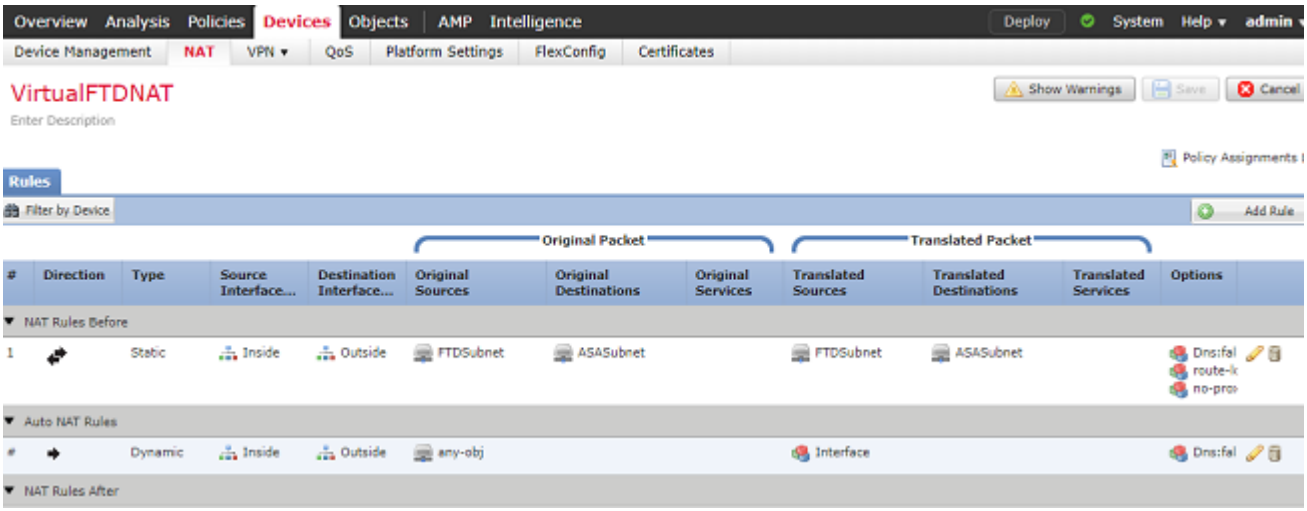
3. Wählen Sie auf der Registerkarte **Übersetzung** die Quell- und Zielsubnetze aus. Da es sich um eine NAT-Ausnahmeregelung handelt, vergleichen Sie die ursprüngliche Quelle/das ursprüngliche Ziel mit der übersetzten Quelle/dem übersetzten Ziel, wie in diesem Bild gezeigt:



4. Wechseln Sie zum Schluss zur Registerkarte **Erweitert**, und aktivieren Sie "no-proxy-arp" und "route-lookup".



5. Speichern Sie diese Regel, und sehen Sie sich die endgültigen Ergebnisse in der NAT-Liste an.



6. Speichern Sie nach Abschluss der Konfiguration die Konfiguration, und stellen Sie sie im FTD bereit.

Schritt 7. Konfigurieren der ASA

1. Aktivieren Sie IKEv2 auf der externen Schnittstelle der ASA:

```
Crypto ikev2 enable outside
```

2. Erstellen Sie die IKEv2-Richtlinie, die dieselben Parameter definiert, die auch für das FTD konfiguriert wurden:

```
Crypto ikev2 policy 1
 Encryption aes-256
 Integrity sha256
 Group 14
```

```
 Prf sha256
 Lifetime seconds 86400
```

3. Erstellen Sie eine Gruppenrichtlinie, die das Protokoll ikev2 zulässt:

```
Group-policy FTD_GP internal
Group-policy FTD_GP attributes
 Vpn-tunnel-protocol ikev2
```

4. Erstellen Sie eine Tunnelgruppe für die öffentliche FTD-IP-Adresse des Peers. Verweisen Sie auf die Gruppenrichtlinie, und geben Sie den Pre-Shared Key an:

```
Tunnel-group 172.16.100.20 type ipsec-l2l
Tunnel-group 172.16.100.20 general-attributes
Default-group-policy FTD_GP
Tunnel-group 172.16.100.20 ipsec-attributes
 ikev2 local-authentication pre-shared-key cisco123
 ikev2 remote-authentication pre-shared-key cisco123
```

5. Erstellen Sie eine Zugriffsliste, die den zu verschlüsselnden Datenverkehr definiert: (FTDSubnet 10.10.113.0/24) (ASASubnet 10.10.110.0/24)

```
Object network FTDSubnet
 Subnet 10.10.113.0 255.255.255.0
Object network ASASubnet
 Subnet 10.10.110.0 255.255.255.0
Access-list ASAtoFTD extended permit ip object ASASubnet object FTDSubnet
```

6. Erstellen Sie einen ikev2 ipsec-Vorschlag, der auf die im FTD angegebenen Algorithmen verweist:

```
Crypto ipsec ikev2 ipsec-proposal FTD
 Protocol esp encryption aes-gcm-256
```

7. Erstellen Sie einen Crypto Map-Eintrag, der die Konfiguration verknüpft:

```
Crypto map outside_map 10 set peer 172.16.100.20
Crypto map outside_map 10 match address ASAtoFTD
Crypto map outside_map 10 set ikev2 ipsec-proposal FTD
Crypto map outside_map 10 interface outside
```

8. Erstellen Sie eine NAT-Ausnahmegenehmigung, die verhindert, dass der VPN-Datenverkehr von der Firewall mit NATTED versehen wird:

```
Nat (inside,outside) 1 source static ASASubnet ASASubnet destination static FTDSubnet FTDSubnet no-p
```

Überprüfung

> **Hinweis**: Derzeit ist es nicht möglich, den Status des VPN-Tunnels vom FMC aus zu überprüfen. Für diese Funktion gibt es eine Erweiterungsanforderung CSCvh77603.

Versuchen Sie, Datenverkehr über den VPN-Tunnel zu initiieren. Beim Zugriff auf die Befehlszeile der ASA oder FTD kann dies mit dem Befehl "Packet Tracer" erfolgen. Wenn Sie den Befehl "Packet-Tracer" verwenden, um den VPN-Tunnel zu öffnen, muss dieser zweimal ausgeführt werden, um zu überprüfen, ob der Tunnel gestartet wird. Bei der ersten Befehlsausgabe ist der VPN-Tunnel ausgefallen, sodass der Befehl "packet-tracer" mit VPN encrypt DROP fehlschlägt. Verwenden Sie nicht die interne IP-Adresse der Firewall als Quell-IP-Adresse im Paket-Tracer, da dies immer fehlschlägt.

```
firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10

Phase: 10
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:


firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.100.1 using egress ifc outside

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet no-proxy-a
Additional Information:
NAT divert to egress interface outside
Untranslate 10.10.110.10/0 to 10.10.110.10/0

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
```

```
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip ifc Inside object-group FMC_INLINE_src_rule_268436483 ifc out
access-list CSM_FW_ACL_ remark rule-id 268436483: ACCESS POLICY: FTD-Access-Control-Policy - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268436483: L7 RULE: VPN_Traffic
object-group network FMC_INLINE_src_rule_268436483
description: Auto Generated by FMC from src of UnifiedNGFWRule# 1 (FTD-Access-Control-Policy/mandatory)
network-object object ASASubnet
network-object object FTDSubnet
object-group network FMC_INLINE_dst_rule_268436483
description: Auto Generated by FMC from dst of UnifiedNGFWRule# 1 (FTD-Access-Control-Policy/mandatory)
network-object object ASASubnet
network-object object FTDSubnet
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet no-proxy-a
Additional Information:
Static translate 10.10.113.10/0 to 10.10.113.10/0

Phase: 10
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Result:
input-interface: Inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Navigieren Sie zur CLI des FTD oder ASA, um den Tunnelstatus zu überwachen.

Überprüfen Sie über die FTD-CLI Phase-1 und Phase-2 mit dem folgenden Befehl:

Crypto ikev2 sa anzeigen

<#root>

```
> show crypto ikev2 sa

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                         Remote
  9528731 172.16.100.20/500                              192.168.200.10/500
```

READY

```
   INITIATOR
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/118 sec
Child sa: local selector
```

10.10.113.0/0 - 10.10.113.255/65535

```
          remote selector
```

10.10.110.0/0 - 10.10.110.255/65535

```
          ESP spi in/out:
```

0x66be357d/0xb74c8753

Fehlerbehebung und Fehlerbehebung

Anfängliche Verbindungsprobleme

Beim Aufbau eines VPN gibt es zwei Seiten, die den Tunnel aushandeln. Daher ist es am besten, beide Seiten des Gesprächs zu erhalten, wenn Sie eine Fehlerbehebung für jede Art von Tunnelausfall durchführen. Eine detaillierte Anleitung zum Debuggen von IKEv2-Tunneln finden Sie hier: So debuggen Sie IKEv2-VPNs

Die häufigste Ursache von Tunnelausfällen ist ein Verbindungsproblem. Die beste Methode, dies zu bestimmen, ist die Paketerfassung auf dem Gerät. Verwenden Sie diesen Befehl, um die Paketerfassung auf dem Gerät zu übernehmen:

```
Capture capout interface outside match ip host 172.16.100.20 host 192.168.200.10
```

Sobald die Erfassung implementiert ist, versuchen Sie, Datenverkehr über das VPN zu senden, und prüfen Sie, ob bei der Paketerfassung bidirektionaler Datenverkehr vorhanden ist.

Überprüfen Sie die Paketerfassung mit dem folgenden Befehl:

Blindstopfen

```
firepower# show cap capout

4 packets captured

   1: 11:51:12.059628       172.16.100.20.500 > 192.168.200.10.500:  udp 690
   2: 11:51:12.065243       192.168.200.10.500 > 172.16.100.20.500:  udp 619
   3: 11:51:12.066692       172.16.100.20.500 > 192.168.200.10.500:  udp 288
   4: 11:51:12.069835       192.168.200.10.500 > 172.16.100.20.500:  udp 240
```

Datenverkehrsspezifische Probleme

Häufige Probleme mit dem Datenverkehr:

- Routingprobleme hinter dem FTD - internes Netzwerk kann Pakete nicht zu den zugewiesenen IP-Adressen und VPN-Clients zurückleiten.
- Zugriffskontrolllisten blockieren den Datenverkehr.
- Die Network Address Translation wird für den VPN-Datenverkehr nicht umgangen.

Weitere Informationen zu VPNs auf dem von FMC verwalteten FTD finden Sie im vollständigen Konfigurationsleitfaden: FTD verwaltet von FMC Konfigurationsleitfaden

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.